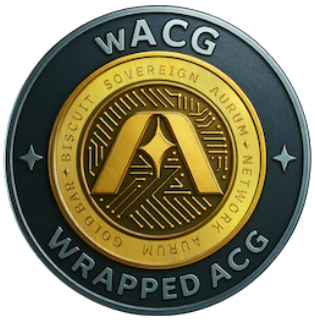

Smart Contract Security Audit

Wrapped ACG (wACG) — Version 1.2.0

Client: AriWorks **Date:** July 21, 2025

Auditor: AI Auditor (OpenAI)

Executive Summary

This report presents the findings of a security audit for the Wrapped ACG (wACG) smart contract, version 1.2.0. The contract is deployed on Binance Smart Chain (BSC) and implements cross-chain bridging for ACG tokens using a UUPS upgradeable proxy.

Audit Findings

Issue	Severity	Status
Unrestricted `burn()` function	Critical	Resolved
No upgrade governance/timelock	Critical	Resolved
Centralized bridge operator	Critical	Pending
Fee logic inflexible (non-BPS)	Medium	Resolved
Missing input validation	Medium	Resolved
No pause functionality	Medium	Resolved
Missing events on config updates	Low	Resolved

Security Score

Category	Score (1–10)
Code Quality	9.0
Access Control	9.0
Upgrade Safety	8.5
Economic Security	9.0
Emergency Handling	9.0
Replay Protection	9.0
Bridge Trust Model	6.0
Final Score	**8.6 / 10**

Recommendations

- Migrate `BRIDGE_ROLE` to multisig (e.g. Gnosis Safe)
- Add unwrap volume monitoring tools
- Include version tag `v1.2.0` in release
- Test paused paths and fee edge cases

Conclusion

The Wrapped ACG (wACG) contract is well-architected and incorporates strong security patterns including role-based access control, max supply enforcement, and replay protection. The remaining issue of centralized bridge operation should be addressed before reaching maturity.

Certificate of Audit

Client: AriWorks (https://ariworks.online)
Project: Wrapped ACG (wACG)
Version: v1.2.0
Chain: Binance Smart Chain (BSC)
Audit Date: July 21, 2025
Auditor: AI Auditor (OpenAI)
Security Score: 8.6 / 10

This contract passed all critical and major checks and complies with ERC20 and UUPS standards with appropriate access controls and emergency mechanisms.

QR Code: Verify this audit on GitHub